SOMOS SEQUENCES, CONTINUED FRACTIONS,AND HYPERELLIPTIC CURVES(Analytic Number Theory and Surrounding Areas)

AUTHOR(S):

VAN DER POORTEN, ALFRED J.

CITATION:

VAN DER POORTEN, ALFRED J.. SOMOS SEQUENCES, CONTINUED FRACTIONS,AND HYPERELLIPTIC CURVES(Analytic Number Theory and Surrounding Areas). 数理解析研究所講究録 2006, 1511: 98-107

ISSUE DATE:

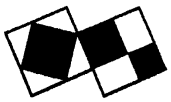
2006-08

URL:

http://hdl.handle.net/2433/58605

数理解析研究所講究録
1511 巻 2006 年 98-107

SOMOS SEQUENCES, CONTINUED FRACTIONS, AND HYPERELLIPTIC CURVES



ceNTRe
Sydney, Australia 2071

ALFRED J. VAN DER POORTEN

ABSTRACT. I detail the continued fraction expansion of the square root of a monic polynomials of even degree. In the quartic and sextic cases I observe explicitly that parameters appearing in the continued fraction expansion yield integer sequences defined by relations instancing sequences of Somos type. Because each step in the expansion corresponds to addition by the divisor at infinity on (the Jacobian of) the relevant curve I recover the link between Somos sequences and the co-ordinates of the multiples of a point on certain curves.

The notes below are in fact the reformatted transcript of a six months later version of the talk I actually gave at the RIMS Meeting on October 20, 2004. Interested readers can click through a more colourful display version of the talk below after downloading it at `http://www.maths.mq.edu.au/~alf/Somos.pdf`.

I am particularly grateful for an incidental remark made to me at the meeting which led me to rethink my method and to find significant simplifications of part of my arguments.

1. TWO SURPRISING ALLEGATIONS

A pseudo-elliptic integral.

$$\int^x \frac{6t}{\sqrt{t^4+4t^3-6t^2+4t+1}}\,dt = \log\Big(x^6+12x^5+45x^4+44x^3-33x^2+43 \\ +(x^4+10x^3+30x^2+22x-11)\sqrt{x^4+4x^3-6x^2+4x+1}\Big).$$

A Somos sequence of width 5. The sequence $(B_h)_{-\infty<h<\infty} = \ldots, 3, 2, 1, 1, 1, 1, 1, 2, 3, 5, 11, 37, 83, \ldots$ is produced by the recursive definition

$$B_{h+3} = (B_{h-1}B_{h+2} + B_hB_{h+1})/B_{h-2}$$

and consists entirely of integers ..... .

Studying the first surprise led me to stumble on to the second.

Typeset May 24, 2005 [16:26].

2000 *Mathematics Subject Classification.* Primary: 11A55, 11G05; Secondary: 14H05, 14H52.

Key words and phrases. continued fraction expansion, function field of characteristic zero, hyperelliptic curve, Somos sequence.

This version of the present lecture was written at Brown University, Providence, Rhode Island where the author held the position of Mathematics Distinguished Visiting Professor, Spring semester, 2005. The author was also supported by his wife and by a grant from the Australian Research Council.

2. Michael Somos' Sequences

Some fifteen years ago, Michael Somos noticed that the two-sided sequence

$$C_{h-2}C_{h+2} = C_{h-1}C_{h+1} + C_h^2,$$

which I refer to as 4-Somos in his honour, apparently takes only integer values if we start from C_{-1}, C_0, C_1, $C_2 = 1$.

Indeed Somos goes on to investigate also the width 5 sequence, $B_{h-2}B_{h+3} = B_{h-1}B_{h+2} + B_hB_{h+1}$, now with five initial 1s, the width 6 sequence $D_{h-3}D_{h+3} = D_{h-2}D_{h+2} + D_{h-1}D_{h+1} + D_h^2$, and so on, testing whether each — when initiated by an appropriate number of 1s — yields only integers. Naturally, he asks: "What is going on here?"

By the way, while 4-Somos (A006720), 5-Somos (A006721), 6-Somos (A006722), and 7-Somos (A006723), do yield only integers; 8-Somos does *not.*

The codes in parentheses refer to Neil Sloane's *On-line encyclopedia of integer sequences.*

Zagier's Comments. Concerning (B_h) — thus 5-Somos — Don Zagier inter alia writes:

"One computes the first few (in my case, 300) terms B_n numerically, studies their numerical growth, and tries to fit this data by a nice analytic expression. One quickly finds that the growth is roughly exponential in n^2, but with some slow fluctuations around this and also with a dependency on the parity of n. This suggests trying the Ansatz $B_n = c_\pm b^n a^{n^2}$, where $(-1)^n = \pm 1$. This is easily seen to give a solution to our recursion if a is the root of $a^{12} = a^4 + 1$, and the numerical value $a = 1.07283$ (approx) does indeed give a reasonably good fit to the data, but eventually fails more and more thoroughly. Looking more carefully, we try the same Ansatz but with $c_\pm$ replaced by a function $c_\pm(n)$ which lies between fixed limits but is almost periodic in n, and this works, but with a new value $a = 1.07425$ (approx) . . . .

Expanding the function $c_\pm(n)$ numerically into a Fourier series, we discover that it is a Jacobi theta function, and since theta functions (or quotients of them) are elliptic functions, this leads quickly to elliptic curves . . . ."

3. Pseudo-Elliptic Integrals

The surprising integral

$$\int^X \frac{6t\,dt}{\sqrt{t^4+4t^3-6t^2+4t+1}} = \log\Big(X^6+12X^5+45X^4+44X^3-33X^2+43 + (X^4+10X^3+30X^2+22X-11)\sqrt{X^4+4X^3-6X^2+4X+1}\Big)$$

is a nice example of a class of *pseudo-elliptic* integrals

$$(*) \qquad \int^X \frac{f(t)dt}{\sqrt{D(t)}} = \log\big(a(X) + b(X)\sqrt{D(X)}\big).$$

Here we take D to be a monic polynomial defined over $\mathbb{Q}$, of even degree $2g+2$, and not the square of a polynomial; f, a, and b denote appropriate polynomials. We suppose a to be nonzero, say of degree m at least $g+1$. We will see that necessarily $\deg b = m-g-1$, that $\deg f = g$, and that f has leading coefficient m.

In our example, $m = 6$ and $g = 1$.

Plainly, if (*) holds then it remains true with $\sqrt{D}$ replaced by its conjugate $-\sqrt{D}$. Adding the two conjugate identities we see that

$$(\dagger) \qquad \int 0\,dt = \log(a^2 - Db^2).$$

Thus $a^2 - Db^2$ is some constant k, and must be nonzero because D is not a square. In other words, $u = a + b\sqrt{D}$ is a nontrivial unit in the function field $\mathbb{Q}(X, \sqrt{D(X)})$; and $\deg a = m$ implies $\deg b = m - g - 1$ is immediate.

Differentiating (†) yields $2aa' - 2bb'D - b^2D' = 0$. Hence $b|aa'$, and since a and b must be relatively prime because u is a unit, it follows that $b|a'$. Set $f = a'/b$, noting that indeed $\deg f = g$ and that f has leading coefficient m because a and b must have the same leading coefficient.*

Moreover,

$$u' = a' + b'\sqrt{D} + bD'/2\sqrt{D} = a' + (2bb'D + b^2D')/2b\sqrt{D} = a' + aa'/b\sqrt{D}.$$

So, remarkably, $u' = f(b\sqrt{D} + a)/\sqrt{D} = fu/\sqrt{D}$.

Thus, to verify (*) it suffices to make the not altogether obvious substitution $u(x) = a + b\sqrt{D}$, of course given that u is a unit of the order $\mathbb{Q}[X, \sqrt{D(X)}]$.

Remark. The case $g = 0$, say $D(X) = X^2 + 2vX + w$, is useful for orienting oneself. Here $(X + v) + \sqrt{D(X)}$ is a unit, of norm $v^2 - w$, and indeed

$$\int \frac{dX}{\sqrt{X^2 + 2vX + w}} = \operatorname{arsinh} \frac{X + v}{\sqrt{w - v^2}} = \log\left(X + v + \sqrt{X^2 + 2vX + w}\right).$$

Notice that $\deg f = 0$ and has leading coefficient 1, as predicted.

4. Units

Units and torsion. The notion *unit* entails that u be trivial at other than infinite *places* (absolute values). That is, the divisor of zeros and poles of the function $u = a + b\sqrt{D}$ is supported only at infinity.

But, speaking plainly, the quartic $C : Y^2 = X^4 + 4X^3 - 6X^2 + 4X + 1$ has two points at infinity, which I shall call S, and O — the latter being the zero of the group law on the elliptic curve C. In general, for $C : Y^2 = D(X)$ of genus g, I had best speak of the point $S - O$ on the Jacobian of the hyperelliptic curve C.

Whatever, there is a positive integer m so that $m(S - O)$ is the divisor of the unit u, showing that $S - O$ is a *torsion point* of order m on $\mathrm{Jac}(C)$.

Units in quadratic fields and continued fractions. One finds a unit u in the domain $\mathbb{Q}[X, Y]$ by studying the continued fraction expansion of $Y = \sqrt{D(X)}$. The principle is that a period of the expansion produces a unit and, conversely, the existence of a unit entails the periodicity of the continued fraction expansion.

Thus — because periodicity is equivalent to torsion at infinity — each step in the continued fraction expansion of Y must somehow add some multiple of the divisor at infinity. This fact is nicely 'explicited' by Bill Adams and Mike Razar (1981).

*That common coefficient is 1 without loss of generality since we may freely choose the constant produced by the indefinite integration.

It's pretty obvious that torsion at infinity is unusual *in characteristic zero.* So periodicity of the expansion of Y must therefore be *exceptional.*

In the numerical case, and for congruence function fields, periodicity is always forced by the box principle. But, over an infinite field, there are infinitely many polynomials of bounded degree .... Periodicity *is* rare happenstance.

5. Continued Fraction of the Square Root of a Polynomial

Set $Y^2 = D(X)$ where $D \neq \square$ is a monic polynomial of degree $2g+2$. Then we may write

$$D(X) = \big(A(X)\big)^2 + 4R(X)\,,$$

where A is the polynomial part of the square root Y of D and $4R$, with $\deg R \leq g$, is the remainder. We then take

$$Y = A\big(1 + 4R/A^2\big)^{1/2} = A(X) + c_1X^{-1} + c_2X^{-2} + \cdots$$

thereby viewing Y as an element of $K((X^{-1}))$, Laurent series in the variable $1/X$. Here we ask only that the base field K be infinite.

However, below we deal with the quadratic irrational function Z defined by

$$(\ddagger) \qquad \mathcal{C} : Z^2 - AZ - R = 0\,.$$

Then $\deg Z = \deg A = g+1$, while its conjugate satisfies $\deg \overline{Z} < 0$. Note that Z makes sense in arbitrary characteristic, including characteristic two.

Now, for $\ldots, -1, h = 0, 1, 2, \ldots,$ set

$$Z_h = (Z + P_h)/Q_h\,,$$

where P_h and Q_h are polynomials satisfying $\deg P_h \leq g-1$, $\deg Q_h \leq g$ and Q_h divides the norm $(Z+P_h)(\overline{Z}+P_h)$.

Then, $\deg Z_h > 0$ and $\deg \overline{Z}_h < 0$ — one says that Z_h is *reduced* — and the $K[X]$-module $\langle Q_h, Z+P_h\rangle$ is in fact an ideal of the domain $K[X,Z]$.

Finally, denote by a_h the polynomial part of Z_h. Then the continued fraction expansion of, say, Z_0 is a sequence of lines (or steps)

$$(Z+P_h)/Q_h = a_h - (\overline{Z}+P_{h+1})/Q_h \quad \text{in brief:} \quad Z_h = a_h - \overline{R}_h\,,$$

where, $-Q_h/(\overline{Z}+P_{h+1}) = (Z+P_{h+1})/Q_{h+1}$. Necessarily

$$P_h + P_{h+1} + A = a_hQ_h \quad \text{and} \quad (Z+P_{h+1})(\overline{Z}+P_{h+1}) = -Q_hQ_{h+1}\,,$$

and one easily verifies that the conditions on the P_h and Q_h are sustained.

There is a minor miracle. Because the *complete quotients* Z_h all are reduced it follows that also all the R_h are reduced. Thus the *partial quotients* a_h, which begin life as the polynomial parts of the Z_h, *also are* the polynomial parts of the R_h.

Thus also the 'conjugate line'

$$R_h = (Z+P_{h+1})/Q_h = a_h - (\overline{Z}+P_h)/Q_h = a_h - \overline{Z}_h$$

is a line in an admissible continued fraction expansion, explaining why I can refer to the original expansion as *bi-directional* infinite.

Given that the base field K is infinite, I assert that a generic choice of P_0 and Q_0 is so that *all* the a_h are linear — equivalently, so that all the Q_h are of degree g — indeed, a teeny bit less obviously, so that all the P_h are of their maximal

degree $g-1$. That's so because the probability of an element of K being zero — *is* zero.

If one prefers, a *generic* divisor of C is defined by a g-tuple of elements of an algebraic extension of K.

I should point out that any actual expansion is *very* messy. I give the list of partial quotients of two very different examples.

$$\sqrt{X^4-2X^3+3X^2+2X+1}+(X^2-X+1)$$
$$=\overline{[2(X^2-X+1)\,,\ \tfrac{1}{2}X-\tfrac{1}{2}\,,\ 2X-2\,,\ \tfrac{1}{2}X^2-\tfrac{1}{2}X+\tfrac{1}{2}\,,\ 2X-2\,,\ \tfrac{1}{2}X-\tfrac{1}{2}]}$$

Here, I've lazily copied the expansion of $2Z$ in a periodic case (so, there's a pseudo-elliptic integral with $D=X^4-2X^3+3X^2+2X+1$). Note that the *quasi-period* already supplies a unit. In fact

$$\int^X \frac{4t-1}{\sqrt{t^4-2t^3+3t^2+2t+1}}\,dt$$
$$=\log\bigl(X^4-3X^3+5X^2-2X+(X^2-2X+2)\sqrt{X^4-2X^3+3X^2+2X+1}\,\bigr).$$

On the other hand, if we replace D by $D+1$ then we obtain a generic expansion nicely illustrating the behaviour of Néron–Tate height.

$$\sqrt{X^4-2X^3+3X^2+2X+2}+(X^2-X+1)$$
$$=[2(X^2-X+1)\,,\ \tfrac{1}{2}X-\tfrac{5}{8}\,,\ \tfrac{32}{21}X-\tfrac{344}{441}\,,\ -\tfrac{9261}{7936}X-\tfrac{2903079}{1968128}\,,$$
$$-\tfrac{488095744}{2572789149}X+\tfrac{162169331891200}{340354276521121}\,,\ -\tfrac{21440698686186129}{1136033082245120}X+\tfrac{16653223342299891329867}{42646681907481804800}\,,$$
$$-\tfrac{160095643880686866952192000}{88607770352600487715818861}X-\tfrac{33719996766956576002150497085030400}{2563513159391015395122201711798263641}\,,$$
$$\tfrac{8008319835604918899934138279552547329396 1}{9759682070832359890985005871634841600 00}X$$
$$-\tfrac{2553683006740627824207318164745239446373641775460 99}{126790742288717260953237768784696128348471951360 00}\,,$$
$$\tfrac{4117934429867578468642904208184426566140181398969531780640000}{503230723831903952989142036290969243284758393383295955214733129}X$$
$$-\tfrac{26784291200643719113416904554352830551520629654059483043111859170312192000 0}{2295347473317007513604838832081344217172192053169949881862822066226067080592 1}\,,\ \ldots\ldots]$$

Even a computer chokes on numbers growing at such a pace.

6. The Continued Fraction Expansions

In the course of studying continued fraction expansions

$$(Z+P_h)/Q_h=a_h-(\overline{Z}+P_{h+1})/Q_h\,,\quad h\in\mathbb{Z}$$

in quadratic function fields I eventually learned by experience that the various parameters detailing the P_h and Q_h are best described in terms of the leading coefficients d_h, say, of the polynomials P_h.

Denote a typical zero of Q_h by ω_h and recall the recursion relations

$$P_h+P_{h+1}+A=a_hQ_h\quad\text{and}$$
$$-Q_hQ_{h+1}=(Z+P_{h+1})(\overline{Z}+P_{h+1})=-R+P_{h+1}(A+P_{h+1})\,.$$

Thus $P_h(\omega_h)+P_{h+1}(\omega_h)+A(\omega_h)=0$ and so $R(\omega_h)=-P_{h+1}(\omega_h)P_h(\omega_h)$.

Hence $Q_h(X)$ divides $R(X)+P_{h+1}(X)P_h(X)$, and so

$$C_h(X)/u_h=\bigl(R(X)+P_{h+1}(X)P_h(X)\bigr)/Q_h(X)$$

defines a polynomial C_h. Here u_h denotes the leading coefficient of Q_h. It's useful that $\deg C_h = \max\bigl(g, 2(g-1)\bigr) - g$; so $\deg C_h = 0$ if $g = 1$ or $g = 2$.

Now suppose that $R(X) = u(X^2 - vX + w)$ if $g = 2$ and $R(X) = u(X - w)$ if $g = 1$ (and recall that d_h is the leading coefficient of $P_h(X)$). It follows that, identically, $C_h(X) = u$ if $g = 1$ and $C_h(X) = d_h d_{h+1} + u$ if $g = 2$.

It also follows from $Q_h(\omega_h) = 0$ *that, for* $h \in \mathbb{Z}$, $\bigl(\omega_h, -P_h(\omega_h)\bigr)$ *specifies a sequence* (M_h) *of divisors on the Jacobian of the curve* $\mathcal{C} : Z^2 - AZ - R = 0$.

We may set $M_h = M + S_h$ (so $M = M_0$). It then turns out that $S_h = hS$ — with S the class of the divisor at infinity. In other words, *each step of the continued fraction expansion is just addition of the divisor at infinity.*

As for our discussion: If $g = 2$ then, if $P_h(\varepsilon_h) = 0$,

$$C_h Q_h(\varepsilon_h) = u_h R(\varepsilon_h) \quad \text{and so} \quad C_{h-1} C_h Q_{h-1}(\varepsilon_h) Q_h(\varepsilon_h) = u_{h-1} u_h R(\varepsilon_h)^2 .$$

From the recursion formulæ, $u_{h-1} u_h = -d_h$, and $Q_{h-1}(\varepsilon_h) Q_h(\varepsilon_h) = R(\varepsilon_h)$. Hence $C_{h-1} C_h = (d_{h-1} d_h + u)(d_h d_{h+1} + u) = R(\varepsilon_h)$, a formula that seemed inexplicably miraculous when I first stumbled upon it. Sadly, my taming it has not yet been enough for me fully to understand the $g = 2$ case.

7. The elliptic case

When $g = 1$ we have $\deg P_h = 0$ and set $P_h = d_h$, and $\deg Q_h = 1$, say with $Q_h(X) = u_h(X - w_h)$. We have $\deg A = 2$ and set, say, $R = u(X - w)$.

Happily, the birational transformation $U = Z$, $V - u = XZ$, transforms our quartic curve into a cubic model passing through the origin

$$\mathcal{E} : V^2 - uV = \text{monic cubic in } U \text{ with zero constant term};$$

the *points* $(w_h, -d_h)$ on $\mathcal{C}$ become $(-d_h, u - w_h d_h)$ on $\mathcal{E}$. The point S is now $(0, 0)$. It is then easy to use the continued fraction recursion formulæ to verify explicitly that $S_h = hS$.

We have $-R(w_h) = d_h d_{h+1}$, $C_h = u$ and that $-C_{h-1} C_h Q_{h-1}(w) Q_h(w)$ is both $u^2 P_h(w)\bigl(A(w) + P_h(w)\bigr)$ and $-u_{h-1} u_h d_{h-1} d_h^2 d_{h+1}$. Thus

$$d_{h-1} d_h^2 d_{h+1} = u^2\bigl(d_h + A(w)\bigr);$$

a recusion formula involving the d_h only. But, the d_h are very messy ... .

The $-d_h$ are in fact U co-ordinates of points on $\mathcal{E}$ (specifically, of the points $M + hS$); therefore they are rationals whose denominators A_h^2, say, are the squares of integers. Accordingly, define a sequence (A_h) by

$$A_{h-1} A_{h+1} = d_h A_h^2 .$$

Conveniently, this immediately yields $A_{h-2} A_{h+2} = d_{h-1} d_h^2 d_{h+1} A_h^2$. So

$$d_{h-1} d_h^2 d_{h+1} = v^2\bigl(d_h + A(w)\bigr) \quad \text{is} \quad A_{h-2} A_{h+2} = v^2 A_{h-1} A_{h+1} + v^2 A(w) A_h^2 ,$$

showing that *all* integer Somos 4 sequences come from (at most quadratic twists of) rational elliptic curves.

A careful look (for example: the theses of Rachel Shipsey and of Christine Swart) at the behaviour of points $M + hS$ on an elliptic curve confirms that the A_h will all be $\mathcal{S}$-integers — with the primes of the finite set $\mathcal{S}$ coming from the factors of the initial values A_0, A_1, A_2, A_3 and the denominators of v and $A(w)$.

As it happens, a combinatorial result — a corollary of Fomin and Zelevinsky's theory of *cluster algebras* — guarantees that elements of Somos 4, ..., Somos 7

sequences are Laurent polynomials in the initial values and with coefficient ring polynomials in the coefficients of the defining recursion.

Somos 5 sequences also come from elliptic curves. It's easy to see that also

$$A_{h-1}A_{h+2} = d_h d_{h+1} A_h A_{h+1}\,,$$

and now the observation that

$$d_{h+1}d_h + u^2/d_h + d_h d_{h-1}$$

is independent of h; that is, it is a *discrete integral* of the difference equation for the d_h, readily yields an identity providing the *width* 5 recursion

$$A_{h-2}A_{h+3} = -u^2 A(w) A_{h-1}A_{h+2} + u^3\big(u + 2wA(w)\big)A_h A_{h+1}.$$

A Somos 5 may be a Somos 4. In any case, its two subsequences (A_{2h+1}) and (A_{2h}) are different Somos 4 sequences deriving from the one elliptic curve and addition by $S_{\mathcal{E}} = (0,0)$ but with initial translations M differing by $\frac{1}{2}S$.

Elliptic Divisibility Sequences. Now consider the *singular* case, $M = O$: thus the continued fraction expansion of Z itself. It will be convenient to write e in place of d, and — in honour of Morgan Ward — (W_h) in place of (A_h). A brief computation reveals $a_0(X) = A$, $e_1 = 0$, $Q_1(X) := u(X - w)$, $e_2 = -A(w)$, sufficing — using the recursion for the sequence (d_h), it being independent of M — to set $W_1 = 1$, $W_2 = u$, leading to $W_3 = -u^2 A(w)$, $W_4 = -u^4\big(u + 2wA(w)\big)$, ...

We notice that in fact (W_h) supplies the coefficients in

$$A_{h-2}A_{h+2} = W_2^2 A_{h-1}A_{h+1} - W_1 W_3 A_h^2\,.$$

Remarkably, Ward introduces his sequence (W_h) in effect as satisfying $W_{-h} = -W_h$ and the multi-recursion

$$W_n^2 W_{h-m}W_{h+m} = W_m^2 W_{h-n}W_{h+n} - W_{m-n}W_{m+n}W_h^2\,.$$

Yet, the special case $n = 1$, $m = 2$, and the values W_1, W_2, W_3, W_4 already determine the sequence.

Ward proves the coherence of his definition by showing there does exist a solution sequence defined in terms of Weierstrass σ-functions.

Recently, Christine Swart and I re-explored this matter and found a direct proof that for all integers m and n

$$W_n^2 A_{h-m}A_{h+m} = W_m^2 A_{h-n}A_{h+n} - W_{m-n}W_{m+n}A_h^2\,.$$

Our argument relies on the amusingly symmetrical identity

$$(d_{h-1} - e_m)d_h^2(d_{h+1} - e_m) = (e_{m-1} - d_h)e_m^2(e_{m+1} - d_h)\,.$$

We have a similar argument and analogous result in the odd gap case.

Andy Hone, I comment on his work below, reacted to our work by giving a direct proof of our results in terms of identities in Weierstrass σ-functions.

Elliptic Division Polynomials. I insisted that the cubic model $\mathcal{E}$ of our elliptic curve contain $(0,0)$. In fact we may suppose we had obtained our $\mathcal{E} = \mathcal{E}(x,y)$ from a more general elliptic curve by translating a notional point $S = (x,y)$ on it to the origin. Then the coefficients of $\mathcal{E}$ are polynomials in x and y and with coefficients polynomials in the original coefficients defining the curve.

This makes the W_h polynomials in x and y. More, if and only if $S = (a,b)$ is a torsion point of order m on $\mathcal{E}$ then $mS = 0$, and $W_m(a,b) = 0$.

It follows that the polynomial $W_h(x,y)$ is the h-th *division polynomial.* That inter alia entails $\gcd\big(W_r(x,y), W_s(x,y)\big) = W_{\gcd(r,s)}(x,y)$, explaining the division properties of the $W_h(0,0)$ and — conversely — the rapid growth of the coefficients of the division polynomials.

By the way, Rachel Shipsey proves directly that if $W_1 = 1$ and $W_2 | W_4$ then $r|s$ entails $W_r | W_s$; hence: elliptic *divisibility* sequence.

4-Somos: Suppose $(C_h) = (\dots, 2, 1, 1, 1, 1, 2, 3, 7, \dots)$ with $C_{h-2}C_{h+2} = C_{h-1}C_{h+1} + C_h^2$. My formulaire quickly reveals that $u = \pm 1$, $w = \mp 2$, $A(w) = 1$, and thus that (C_h) arises from

$$Y^2 = (X^2 - 3)^2 + 4(X - 2) \quad \text{with } M = (1,0);$$

equivalently from $\mathcal{E} : V^2 - V = U^3 + 3U^2 + 2U$ with $M_{\mathcal{E}} = (-1,1)$.

5-Somos: The case $(B_h) = (\dots, 2, 1, 1, 1, 1, 1, 2, 3, 5, 11, \dots)$ with $B_{h-2}B_{h+3} = B_{h-1}B_{h+2} + B_hB_{h+1}$ is trickier. One needs to define $c_hB_{h-1}B_{h+1} = e_hB_h^2$ with c_hc_{h+1} independent of h.

One finds that (B_h) arises from

$$Y^2 = (X^2 - 29)^2 - 4 \cdot 48(X + 5) \quad \text{with } M = (-3,4);$$

equivalently from $\mathcal{E} : V^2 + UV + 6V = U^3 + 7U^2 + 12U$ with $M_{\mathcal{E}} = (-2,-2)$. The fact $\gcd(6,12) \neq 1$ at first hit me for six but was eventually overcome.

By symmetry each respective M is a point of order 2 on its curve.

8. Genus $g \geq 2$

There surely are analogous results for higher genus curves. Indeed, more than a dozen years ago, David Cantor showed for higher genus hyperelliptic curves that there are analogues of the division polynomials satisfying relations given by certain Kronecker–Hankel determinants.

My program falters almost immediately, though I can handle curves $Z^2 - AZ - R = 0$ with $\deg A = 3$ provided that $\deg R = -v(X - W)$ is linear (I put $u = 0$ in the general $R(X) = u(X^2 - vX + w) \dots$).

In that case I find that (*if* $d_{h-1}d_hd_{h+1} \neq 0$)

$$d_{h-2}d_{h-1}^2d_h^3d_{h+1}^2d_{h+2} = v^2d_{h-1}d_h^2d_{h+1} - v^3A(w),$$

yielding a width 6 relation

$$A_{h-3}A_{h+3} = v^2A_{h-2}A_{h+2} - v^3A(w)A_h^2.$$

Others can do worse, and better. Andy Hone had noted that all is revealed by the readily checked assertion that there are constants α and β so that

$$\big(\wp(x+y) - \wp(y)\big)\big(\wp(x) - \wp(y)\big)^2\big(\wp(x-y) - \wp(y)\big) = -\alpha\big(\wp(x) - \wp(y)\big) + \beta,$$

given $y \in \mathbb{C}$; particularly that $\alpha = \wp'(y)^2$, $\beta = \wp'(y)^2(\wp(2y) - \wp(y))$.

Notice that this is just my relation on the $-d_h$ (it also is a remark of Nelson Stephens basic to Christine Swart's thesis).

Hone *et al* have found an analogous relation for Kleinian σ-functions in genus 2 and have used it to obtain a Somos 8 (*not* the most general Somos 8) relation corresponding to curves $Y^2 =$ a quintic in X.

My guess, based on Cantor's results and my partial ones, is that for $g = 2$ the *minimal* relation in fact has width 6, but is cubic — rather than quadratic as in the Somos cases.

That guess coheres with the opinion of Noam Elkies that the special cases

$$Z^2 - AZ + v(X - w) = 0$$

with $\deg A = g + 1$ *do* yield Somos relations of width $2g + 2$.

A cute example à la Somos. Whatever, I can show such things as that the example $(T_h) = (\ldots, 2, 1, 1, 1, 1, 1, 1, 2, 3, 4, 8, 17, 50, \ldots)$, with

$$T_{h-3}T_{h+3} = T_{h-2}T_{h+2} + T_h^2,$$

may be thought of as arising from the points (thus, divisor classes) $\ldots$, $M - S$, M, $M + S$, $M + 2S$, $\ldots$ on the Jacobian of the genus 2 hyperelliptic curve

$$\mathcal{C} : Y^2 = (X^3 - 4X + 1)^2 + 4(X - 2).$$

Here S is the class of the divisor at infinity and M is instanced by the divisor defined by the pair of points $(\varphi, 0)$ and $(\overline{\varphi}, 0)$: where φ is the golden ratio, a happenstance that will please adherents to the cult of Fibonacci. The symmetry dictates that $M - S = -M$ so $2M = S$ on $\mathrm{Jac}(\mathcal{C})$.

References

[1] Adams, William W. and Razar, Michael J. (1980). Multiples of points on elliptic curves and continued fractions. *Proc. London Math. Soc.* **41**, 481–498. MR 591651.

[2] Braden, Harry W., Enolskii, Victor Z., and Hone, Andrew N. W. (2005). Bilinear recurrences and addition formulæ for hyperelliptic sigma functions'. 15pp: at `http://www.arxiv.org/math.NT/0501162`.

[3] Cantor, David G. (1987). Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.* **48**.177, 95–101. MR 866101.

[4] Cantor, David G. (1994). On the analogue of the division polynomials for hyperelliptic curves. *J. für Math.* (Crelle), **447**, 91–145. MR 1263171.

[5] Everest, Graham, van der Poorten, Alf, Shparlinski, Igor, and Ward, Thomas (2003). *Recurrence Sequences*. Mathematical Surveys and Monographs 104, American Mathematical Society, xiv+318pp. MR 1990179.

[6] Fomin, Sergey and Zelevinsky, Andrei (2002). The Laurent phenomenon. *Adv. in Appl. Math.*, **28**, 119–144. MR 1888840. Also 21pp: at `http://www.arxiv.org/math.CO/0104241`.

[7] Gale, David (1991). The strange and surprising saga of the Somos sequences. *The Mathematical Intelligencer* **13**.1 (1991), 40–42; Somos sequence update. *Ibid.* **13**.4, 49–50.

[8] Hone, A. N. W. (2005). Elliptic curves and quadratic recurrence sequences. *Bull. London Math. Soc.* **37**, 161–171.

[9] Lauter, Kristin E. (2003). The equivalence of the geometric and algebraic group laws for Jacobians of genus 2 curves. *Topics in algebraic and noncommutative geometry* (Luminy/Annapolis, MD, 2001), 165–171, *Contemp. Math.*, **324**, Amer. Math. Soc., Providence, RI. MR 1986121.

[10] van der Poorten, Alfred J. (2004). Periodic continued fractions and elliptic curves. In *High Primes and Misdemeanours*: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Institute Communications **42**, American Mathematical Society, 353–365. MR 2076259.

[11] VAN DER POORTEN, ALFRED J. (2005). Elliptic curves and continued fractions. *J. Integer Sequences* **8**, article 05.2.5; also 12pp: at `http://arxiv.org/math.NT/0403225`.

[12] VAN DER POORTEN, ALFRED J. (2005). Curves of genus 2, continued fractions, and Somos sequences. 6pp: at `http://arxiv.org/math.NT/0412372`.

[13] VAN DER POORTEN, ALFRED J. and SWART, CHRISTINE S. (2005). Recurrence relations for elliptic sequences: every Somos 4 is a Somos k. 7pp: `http://arxiv.org/math.NT/0412293`.

[14] PROPP, JIM. *The Somos Sequence Site.* `http://www.math.wisc.edu/~propp/somos.html`.

[15] SHIPSEY, RACHEL (2000). *Elliptic divisibility sequences*, Phd Thesis, Goldsmiths College, University of London. `http://homepages.gold.ac.uk/rachel/`.

[16] SLOANE, NEIL. *On-Line Encyclopedia of Integer Sequences.* `http://www.research.att.com/~njas/sequences/`.

[17] SWART, CHRISTINE (2003). *Elliptic curves and related sequences.* PhD Thesis, Royal Holloway, University of London.

[18] WARD, MORGAN (1948). Memoir on elliptic divisibility sequences *Amer. J. Math.* **70**, 31–74. MR 0023275.

[19] ZAGIER, DON (1966). Problems posed at the St Andrews Colloquium, Solutions, 5th day; see `http://www-groups.dcs.st-and.ac.uk/~john/Zagier/Problems.html`.

CENTRE FOR NUMBER THEORY RESEARCH, 1 BIMBIL PLACE, KILLARA, SYDNEY, NSW 2071, AUSTRALIA

Current address: Department of Mathematics, Brown University, Providence, Rhode Island

E-mail address: `alf@math.mq.edu.au (Alf van der Poorten AM)`